UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/648,630	08/25/2003	Ernst B. Carter	EXIT-00101	5318

28960 7590 12/30/2009
HAVERSTOCK & OWENS LLP
162 N WOLFE ROAD
SUNNYVALE, CA 94086

EXAMINER
POWERS, WILLIAM S

ART UNIT	PAPER NUMBER
2434	

MAIL DATE	DELIVERY MODE
12/30/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.	Applicant(s)	
10/648,630	CARTER ET AL.	
Examiner	**Art Unit**	
WILLIAM S. POWERS	2434	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 December 2009*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-45,47-52 and 59-75* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *26-45,47-52,59,60,63-71 and 73-75* is/are allowed.

6)☒ Claim(s) *1-25,61,62 and 72* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application
6) □ Other: _____.

DETAILED ACTION

1. Applicant's arguments filed 12/8/2009 pertaining to claims 1-25, 61, 62 and 72 have been fully considered but they are not persuasive.

2. As to Applicant’s argument that, “Neither Riedel nor Yu, either alone or in combination, discloses the combination recited in Claim 1, including an operating system comprising a kernel to use system-unique data to verify a user to control access to the encrypted data file” (Remarks, p. 14), the Examiner respectfully disagrees. Applicant is directed to the Yu reference, which shows the use of user access control in the kernel space (Yu, p. 4, fig. 1). Yu expands on the access control to show that it is implemented through Mandatory Access Control (MAC) classes. Users are only allowed access to files of other users within the same MAC class (Yu, p. 5, sec. 5.1). This reads on “a kernel to use system-unique data (MAC class) to verify a user to control access to the encrypted data file.” For at least the reasons above, the rejection of the claim limitations is maintained.

3. Applicant’s arguments, see Remarks, filed 12/8/2009, with respect to claims 26-45, 47-52, 59, 60, 63-71 and 73 have been fully considered and are persuasive. The rejection of claims 26-45, 47-52, 59, 60, 63-71 and 73 has been withdrawn.

Response to Amendment

4. The Examiner has stated the below column and line numbers as examples. All columns and line numbers in the reference and the figures are relevant material and Applicant should take the entire reference into consideration upon the reply to this Office Action.

5. Claims 46 and 53-58 have been cancelled.

6. Claims 1, 16, 17, 25, 26, 36, 40, 48, 71 and 73 have been amended.

7. Claims 74 and 75 have been added.

8. Claims 1-45, 47-52 and 59-75 are pending.

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

11. Claims 1-5, 11, 12, 19, 20, 61, 62 and 72 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 7,313,694 to Riedel et al. (hereinafter Riedel) in view of “A Cryptographic File System Supporting Multi-Level Security” by Yu et al. (hereinafter Yu).

As to claim 1, Riedel teaches:

a. A computer system comprising a memory portion containing an encrypted file data (encrypted files are stored) (Riedel, col. 8, lines 24-27) and an operating system (UNIX operating system) (Riedel, col. 4, lines 1-12).

Riedel does not expressly mention the kernel of the operating system, but it is inherent that the operating system has a kernel. However, in an analogous art, teaches implementing an encryption file system at the kernel level to use system-unique data to verify a user to control access to the encrypted data file (The use of user access control in the kernel space as shown in fig. 1. Yu expands on the access control to show that it is implemented through Mandatory Access Control (MAC) classes. Users are only allowed access to files of other users within the same MAC class which reads on system-unique data for verification purposes.) (Yu, pg. 3, sec. 4, pg. 4, fig.1, pg. 5, sec. 5.1).

Therefore, one of ordinary skill in the art at the time the invention was made would have been motivated to implement the secure file system of Riedel with the kernel implementation of Yu in order to operate under the user-level and to support secure data sharing as suggested by Yu (Yu, pg. 2, 3rd full paragraph and pg. 3, sec. 3).

Riedel as modified further teaches:

b. A virtual node configured (data encryption block and encryption decision block are implemented in the vnode layer for encryption and decryption as requested) (Yu, pg. 4, fig. 1 and associated text) to decrypt an encrypted directory entry to determine a location of the encrypted data file (decryption of the filename and the i-node pointer) (Riedel, col. 7, lines 30-49) and to decrypt the encrypted data file to access data file contents contained therein (data files can be encrypted for added security) (Riedel, col. 8, lines 21-27).

As to claim 2, Riedel as modified teaches wherein the kernel comprises an encryption engine configured to encrypt clear data files to generate cipher data files, the encryption engine further configured to decrypt the cipher data files to generate clear data files (as evidenced by the encryption and decryption of data files for additional security) (Riedel, col. 8, lines 21-27).

As to claim 3, Riedel as modified teaches the memory portion is coupled to the encryption engine and configured to store the cipher data files (encrypted data files are stored in the storage system) (Riedel, col. 8, lines 21-27).

As to claim 4, Riedel as modified teaches an encryption engine is configured to encrypt the clear data files and decrypt the cipher data file according to a symmetric key encryption algorithm (Blowfish algorithm is used) (Yu, pg. 4, last paragraph).

As to claim 5, Riedel as modified teaches the symmetric key encryption algorithm is based on a block cipher (block cipher algorithm used) (Yu, pg. 4, last paragraph).

As to claim 11, Riedel as modified teaches the symmetric key encryption algorithm comprises Blowfish (Blowfish is used as a symmetric key encryption algorithm) (Yu, pg. 4, last paragraph).

As to claim 12, Riedel as modified teaches the kernel comprises a UNIX operating system (UNIX operating system) (Riedel, col. 4, lines 1-12).

As to claim 19, Riedel as modified teaches further comprising a secondary device coupled to the memory, wherein the secondary device stores the encrypted data file and is accessed using a file abstraction (The distributed computer system of the patent can be embodied with multiple storage nodes (secondary stores) (Riedel, fig. 1, ref. 106). The UNIX operating system treats files as abstractions as mentioned in Applicant's specification [0084] and UNIX is the operating system used by the Riedel patent) (Riedel, col. 1, lines 14-22 and col. 4, lines 1-12).

As to claim 20, Riedel as modified teaches the secondary device is a backing store (data storage) (Riedel, fig. 1, ref. 106 and associated text).

As to claims 61 and 62, Riedel as modified teaches an encrypted directory with file names and i-nodes (file names and i-nodes are encrypted, the i-nodes include location information) (Riedel, col. 4, lines 1-67).

As to claim 72, Riedel as modified teaches further comprising a plurality of different encryption keys to decrypt corresponding blocks of the data file (different files have different keys or combinations of keys) (Riedel, col. 4, lines 30-55).

12. Claims 6-8, 14 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 7,313,694 to Riedel et al. (hereinafter Riedel) in view of “A Cryptographic File System Supporting Multi-Level Security” by Yu et al. (hereinafter Yu) as applied to claim 1 above, and further in view of US Patent Application Publication No. 2003/0005300 to Noble et al. (hereinafter Noble).

As to claim 6, Riedel as modified does not expressly mention the Rijndael algorithm. However, the Rijndael algorithm is old and well known in the art at the time of Applicant’s invention as evidenced by Noble. Noble teaches the symmetric key encryption algorithm comprises Rijndael algorithm (Noble, [0090]).

Therefore, one of ordinary skill in the art at the time the invention was made would have been motivated to implement the secure file system of Riedel as modified with the use of the Rijndael algorithm in order to take advantage of its excellent performance characteristics as suggested by Noble (Noble, [0090]).

As to claim 7, Riedel as modified teaches the symmetric key encryption algorithm uses a block size of 128 bits (block size of 16 byte) (Noble, [0091]).

As to claim 8, Riedel as modified teaches the symmetric key encryption algorithm uses a key length of 128 bits (key size of 16 byte) (Noble, [0091]).

As to claim 14, Riedel as modified teaches wherein the memory portion comprises a first logical protected memory configured to store encrypted data files and a second logical protected memory configured to store encrypted key data (decryption keys are not stored with the encrypted files) (Riedel, col. 5, line 63-col. 6, line 3) (encrypted keys are stored in memory) (Noble, [0047, 0051-0054]).

As to claim 15, Riedel as modified teaches an encryption key management system configured to control access to the encrypted data files and the encrypted key data (use of authentication token to control access to encrypted files and respective encrypted keys) (Noble, Abstract).

13. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 7,313,694 to Riedel et al. (hereinafter Riedel) in view of “A Cryptographic File System Supporting Multi-Level Security” by Yu et al. (hereinafter Yu) as applied to claim 1 above, and further in view of “A Cryptographic File System for UNIX” by Blaze.

As to claim 9, Riedel as modified does not expressly mention using the DES algorithm. However, in an analogous art, Blaze teaches wherein the symmetric key encryption algorithm comprises a DES algorithm (Blaze, sec. 3, 1st paragraph).

Therefore, one of ordinary skill in the art at the time the invention was made would have been motivated to implement the secure file system of Riedel as modified with the encryption engine of Blaze in order to achieve a secure, transparent encryption/decryption file system as suggested by Blaze (Blaze, Abstract).

14. Claims 10 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 7,313,694 to Riedel et al. (hereinafter Riedel) in view of “A Cryptographic File System Supporting Multi-Level Security” by Yu et al. (hereinafter Yu), and further in view of US Patent Application Publication No. 2003/0005300 to Noble et al. (hereinafter Noble) as applied to claim 5 above, and further in view of US Patent No. 5,903,881 to Schrader et al. (hereinafter Schrader).

As to claim 10, Riedel as modified does not expressly mention the use of the Triple-DES encryption algorithm. However, in an analogous art, Schrader teaches the symmetric key encryption algorithm comprises a Triple-DES algorithm (Schrader, col. 17, lines 12-21).

Therefore, one of ordinary skill in the art at the time the invention was made would have been motivated to implement the secure file system of Riedel as modified with the use of the Triple-DES algorithm of Schrader in order to provide security for transactions as suggested by Schrader (Schrader, col. 17, lines 12-21).

15. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent No. 7,313,694 to Riedel et al. (hereinafter Riedel) in view of “A Cryptographic File System Supporting Multi-Level Security” by Yu et al. (hereinafter Yu) as applied to claim 12 above, and further in view of US Patent No. 5,727,206 to Fish et al. (hereinafter Fish).

As to claim 13, Riedel as modified does not expressly mention the version of UNIX that is used. However, in an analogous art, Fish teaches wherein the UNIX operating system is a System V-Revision (file system operates in a UNIX SVR4 environment) (Fish, col. 12, lines 22-32).

Therefore, one of ordinary skill in the art at the time the invention was made would have been motivated to implement the secure file system of Riedel with the system v-revision UNIX environment of Fish because the use of vnodes makes integration more seamless as suggested by Fish (Fish, col. 12, lines 22-32).

Allowable Subject Matter

16. Claims 26-45, 47-52, 59, 60, 63-71 and 73-75 are found allowable over the prior art for the reasons included in the Remarks of 12/8/2009.

17. Claims 16-18 and 25 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

18. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to WILLIAM S. POWERS whose telephone number is (571)272-8573. The examiner can normally be reached on m-f 8:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571 272 3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/W. S. P./
Examiner, Art Unit 2434

William S. Powers
Examiner
Art Unit 2434

12/23/2009

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2434